REMARKS

Claims 1-20 are pending in the present application and were each rejected in the May 13, 2005 Office Action. No claims have been allowed.

Reconsideration of the claims is respectfully requested.

In Sections 4-11 of the May 13, 2005 Office Action, the Examiner rejected Claims 1-6, 8-14 and 16-19 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,587,684 to *Hsu et al.* (hereafter, "*Hsu*") in view of U.S. Patent No. 6,647,260 to *Dusse et al.* (hereafter, "*Dusse*") and further in view of U.S. Patent No. 6,591,306 to *Redlich et al.* (hereafter, "*Redlich*"). In Sections 12 and 13 of the May 13, 2005 Office Action, the Examiner rejected Claims 7, 15 and 20 under 35 U.S.C. §103(a) as being unpatentable over *Hsu* , *Dusse* and *Redlich* in view of U.S. Patent No. 6,032,043 to *Houde et al.* (hereafter "*Houde*").

In a previous response, Applicants distinguished the current claims over a combination of Hsu, Dusse, and Houde. Those arguments are hereby incorporated by reference herein.

The Applicants respectfully disagree with the Examiner's rejection of Claims 1-20 and direct the Examiner's attention to Claim 1, which recites the unique and non-obvious limitations emphasized below:

> 1. For use in a wireless network comprising a plurality of base stations, each of said base stations capable of communicating with a plurality of mobile stations, a security device coupled by a wireline connection to said wireless network capable of preventing an unprovisioned one of said plurality of mobile stations from accessing an Internet protocol (IP) data network through said wireless network, said security device comprising:
>
> a first controller capable of receiving an IP data packet transmitted by said unprovisioned mobile station, said IP data packet comprising an IP packet header and an IP packet payload, determining from said IP data packet that said unprovisioned

> mobile station is unprovisioned and, in response to said determination, encrypting at least a portion of said IP packet payload to thereby generate an encrypted payload that may be decrypted only by a provisioning server of said wireless network. (emphasis added)

The Applicants respectfully assert that the above-emphasized limitations are not disclosed or even suggested in any one of the *Hsu* reference, the *Dusseu* reference, the *Redlich* reference, or the *Houde* reference, or in any combination of two or more of the *Hsu* reference, the *Dusseu* reference, the *Redlich* reference, and the *Houde* reference.

Independent Claim 1 recites "a security device coupled by a wireline connection to [a] wireless network..., comprising a first controller capable of...encrypting at least a portion of an IP packet payload to thereby generate an encrypted payload that may be decrypted only by a provisioning server of the wireless network." In the October 6, 2004 Office Action, the Examiner acknowledged that the *Hsu* reference, which describes a system in which a wireless telephone encrypts packets for decryption by a provisioning server, does not teach a security device coupled by a wireline connection to a wireless network comprising a first controller capable of encrypting a payload that may be decrypted only by a provisioning server of the wireless network. However, the Examiner asserted that the *Dusse* reference teaches the encrypting of at least a portion of an IP packet payload to thereby generate an encrypted payload that may be decrypted only by a provisioning server of the wireless network, citing *Dusse*, column 7, lines 1-14, as describing a secure communications session between a proxy server and a provisioning server.

The Applicants respectfully assert that the cited passage actually describes an exchange of provisioning content between a mobile device and a provisioning server. The Examiner also cites

column 4, line 66, through column 5, line 14, previously noted by Applicant, which describes a sequence of actions performed by the *Dusse* system when an unprovisioned mobile device is initially turned on. This passage states:

> According to one embodiment of the present invention, mobile device 100 is initially unprovisioned when obtained (e.g., at a retail store or via the mail) by a user. When mobile device 100 is initially turned on a communications session is established with proxy server device 108 and a provisioning application is activated which displays scripts on display screen 102 of mobile device 100 prompting the user to input provisioning related information via user interface 103. The provisioning related information and pre-stored device identification information (also referred to as a provisioning request herein) are forwarded to provisioning server 120 via proxy server device 108 using a secure communications session. The secure communications session is facilitated by a previously stored uniform resource identifier (URI) associated with provisioning server 120 and authentication services provided by proxy server device 108. (*Emphasis added*).

As noted in a previous response, this quoted passage does not clarify whether a secure communication session is established between the proxy server and the provisioning server, or between the provisioning application and the provisioning server. However, subsequent portions of the *Dusse* reference make clear that the secure communication session is established between the provisioning application (in the mobile device) and the provisioning server.

The passage quoted above indicates that the provisioning application is resident in the mobile device: "[A] provisioning application is activated which displays scripts on display screen 102 of mobile device 100 prompting the user to input provisioning related information via user interface 103." *Dusse, col. 5, lines 3-6.* A subsequent passage describing Fig. 2, which illustrates a mobile device, supports this interpretation:

> Hypermedia information 208 is illustrative of the type of an entry screen relating to the provisioning application. Hypermedia information 208 is comprised of a

> plurality of selectable identifiers corresponding to selections available in the provisioning application. . . . The provisioning application allows the user to pick and chose desired device features and services (selections 2 and 3 on screen 204) or to select predetermined device and service configurations (selection 1 on screen 204). *(Dusse, col. 5, lines 51-65)*

Another subsequent passage clarifies that the secure communication session is established between the mobile device and the provisioning server. Figure 7A illustrates the process used by a mobile device to make a provisioning request. The accompanying description states "a secure communications session is established between the requesting mobile device and the provisioning server." *Dusse, col. 8, lines 16-18.*

Thus, the Applicants respectfully submit that the passage of the *Dusse* reference at column 5, lines 1-14, actually teaches that a secure communication session is established between an unprovisioned mobile device and a provisioning server, as is also taught in the *Hsu* reference. Nor does the *Houde* reference overcome this shortcoming of the *Hsu* and *Dusse* references. Thus, the Applicants respectfully submit that "a security device coupled by a wireline connection to [a] wireless network..., comprising a first controller capable of...encrypting at least a portion of an IP packet payload...that may be decrypted only by a provisioning server of the wireless network," as recited in independent Claim 1, is not disclosed, suggested, or even hinted at in the *Hsu*, *Dusse* and *Houde* references, alone or in combination.

The Examiner cites *Redlich* for the teaching of a "method of encrypting communication between network elements." Indeed, *Redlich* does mention that an IP "tunnel" between network elements can be encrypted.

However, even this three-way combination fails to meet the plain limitation found in the independent claims: "determining from said IP data packet that said unprovisioned mobile station is unprovisioned and, in response to said determination, encrypting at least a portion of said IP packet payload to thereby generate an encrypted payload that may be decrypted only by a provisioning server of said wireless network". Nothing in this combination of references, or any of the cited art individually, teaches or suggests a controller in a base station that encrypts at least a portion of an IP packet payload that may be decrypted only by a provisioning server of the wireless network in response to determining from the IP data packet that a mobile station is unprovisioned. In fact, this responsive relationship, as found in the claims, is completely omitted from the analysis in section 6 of the outstanding Office Action. The Examiner has not even made a *prima facie* showing that this claimed relationship is taught or suggested by any art of record, alone or in combination.

Furthermore, the Office Action states that the person of ordinary skill in the art would have been motivated to modify the system of the *Hsu* reference by the teaching of the *Dusse* reference in order to protect sensitive information such as credit card information from interception. The Applicants respectfully submit that the *Hsu* reference teaches the establishment of a secure link between a digital telephone and a provisioning server, thereby protecting all information transmitted over the link. Thus, the person of ordinary skill would have no need to modify the system of the *Hsu* reference according to the teaching of the *Dusse* reference in order to protect sensitive information from interception.

The Examiner's stated motivation for combining *Hsu* and *Dusse* with *Redlich*, for "providing a level of privacy that is usually associated with a physical wire" is similarly baseless, since *Hsu* already teaches the establishment of a secure link between a digital telephone and a provisioning server, thereby protecting all information transmitted over the link, so that a person of ordinary skill in the art would have no need to modify *Hsu* according to *Redlich* to further protect just a portion of the communication that is already protected. As such, the Office Action fails to show some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the cited references, as required to establish a *prima facie* case of obviousness.

For these reasons, independent Claims 1, 9 and 17 present patentable subject matter over the *Hsu*, *Dusse,* and *Redlich* references, and over the *Houde* reference as well, as described above and in the previous response. Additionally, dependent Claims 2-8, 10-16, and 18-20, which depend from Claims 1, 9 and 17, respectively, contain all of the unique and novel limitations recited in independent Claims 1, 9 and 17. Claims 2-8, 10-16, and 18-20 are therefore patentable over the *Hsu*, *Dusse, Redlich,* and *Houde* references.

SUMMARY

For the reasons given above, the Applicants respectfully request reconsideration and allowance of pending claims and that this Application be passed to issue. If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this Application, the Applicants respectfully invite the Examiner to contact the undersigned at the telephone number indicated below or at ***jmockler@davismunck.com***.

The Commissioner is hereby authorized to charge any additional fees connected with this communication or credit any overpayment to Deposit Account No. 50-0208.

Respectfully submitted,

DAVIS MUNCK, P.C.

Date: 15 August 2005

John T. Mockler
Registration No. 39,775

P.O. Drawer 800889
Dallas, Texas 75380
Phone: (972) 628-3600
Fax: (972) 628-3616
E-mail: *jmockler@davismunck.com*